| FISMA | | | | |
|---|---|---|---|---|
| 2004 Report Grading Elements | | | | |
| | Report Grading Element | | | FY04 Possible Points |
| | Total possible points: | | | 100 |
| **A. Annual Testing** | | | | **20** |
| **1** | **The percentage of the agency's programs and systems reviewed, including contractor operations or facilities in FY04 by CIOs and IGs were:** | | | **12** |
| | **i)** | The percentage of agency systems reviewed in FY04 was: | | **4** |
| | | a | Between 90 and 100% | 4 |
| | | b | Between 75 and 89% | 3 |
| | | c | Between 60 and 74% | 2 |
| | | d | Between 45 and 59% | 1 |
| | | e | 44% and less | 0 |
| | **ii)** | The percentage of contractor operations or facilities reviewed in FY04 was: | | **8** |
| | | a | Between 90 and 100% | 8 |
| | | b | Between 75 and 89% | 6 |
| | | c | Between 60 and 74% | 4 |
| | | d | Between 45 and 59% | 2 |
| | | e | 44% and less | 0 |
| **2** | **The degree to which agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency are adequately secure and meet policy requirements?** | | | **4** |
| | | a | Between 96 and 100% | 4 |
| | | b | Between 81and 95% | 3 |
| | | c | Between 71 and 80% | 2 |
| | | d | Between 51and 70% | 1 |
| | | e | 50% and less | 0 |
| **3** | **The degree to which the agency used the NIST self-assessment guide or equivalent methodology to conduct its reviews?** | | | **3** |
| | | a | Between 81 and 100% | 3 |
| | | b | 80% and less | 0 |
| **3a** | **The agency has appointed a senior agency information security officer that reports directly to the CIO.** | | | **1** |
| | | a | Yes | 1 |
| | | b | No | 0 |

| FISMA<br>2004 Report Grading Elements | | | | |
|---|---|---|---|---|
| | Report Grading Element | | | FY04 Possible Points |
| **B. Plan of Action and Milestones (POA&M)** | | | | **15** |
| **4** | **Has the agency developed POA&Ms for each significant deficiency identified in FY04?** | | | **1** |
| | | a | Yes | 1 |
| | | b | No | 0 |
| **5** | **Has the agency developed, implemented, and managing an agency-wide plan of action and milestone process. (OIG Assessment)** | | | **14** |
| | **i)** | **Known IT security weaknesses, from all components, are incorporated into the POA&M.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | **ii)** | **Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | **iii)** | **Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.** | | **1** |
| | | a | Between 96 and 100% | 1 |
| | | b | Between 51and 95% | 0.5 |
| | | c | 50% and less | 0 |
| | **iv)** | **CIO develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | **v)** | **CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |

| FISMA | | | | |
|---|---|---|---|---|
| 2004 Report Grading Elements | | | | |
| Report Grading Element | | | | FY04 Possible Points |
| | | e | 50% and less | 0 |
| | vi) | **OIG has access to POA&Ms as requested.** | | **1** |
| | | a | Between 96 and 100% | 1 |
| | | b | Between 51and 95% | 0.5 |
| | | c | 50% and less | 0 |
| | vii) | **The OIG's findings are incorporated into the POA&M process.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | viii) | **The agency's POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |

| FISMA | | | | |
|---|---|---|---|---|
| 2004 Report Grading Elements | | | | |
| | | Report Grading Element | | FY04 Possible Points |
| **C. Certification and Accreditation (C&A)** | | | | **20** |
| **6** | | **The percentage of systems that have been certified and accredited is:** | | **12** |
| | **i)** | a | Between 90 and 100% | 12 |
| | | b | Between 75 and 89% | 8 |
| | | c | Between 60 and 74% | 4 |
| | | d | Between 45 and 59% | 2 |
| | | e | 44% and less | 0 |
| | | **The percentage of systems that have the costs of their security controls integrated into the life cycle of the system is:** | | **2** |
| | **ii)** | a | Between 90 and 100% | 2 |
| | | b | Between 75 and 89% | 1.5 |
| | | c | Between 60 and 74% | 1 |
| | | d | Between 45 and 59% | 0.5 |
| | | e | 44% and less | 0 |
| | | **The percentage of systems whose security controls have been tested and evaluated in the last year is:** | | **2** |
| | **iii)** | a | Between 90 and 100% | 2 |
| | | b | Between 75 and 89% | 1.5 |
| | | c | Between 60 and 74% | 1 |
| | | d | Between 45 and 59% | 0.5 |
| | | e | 44% and less | 0 |
| | | **The percentage of systems that have a contingency plan that has been tested in the past year is:** | | **4** |
| | **iv)** | a | Between 90 and 100% | 4 |
| | | b | Between 75 and 89% | 3 |
| | | c | Between 60 and 74% | 2 |
| | | d | Between 45 and 59% | 1 |
| | | e | 44% and less | 0 |
| | | **OIG Assessment of the Certification and Accreditation Process** | | **0** |
| | **v)** | | **OIG C&A Evaluation** | |
| | | a | Excellent, Good, Satisfactory (No Deduction from C&A score in question 6i ) | 0 Deductions |
| | | b | Poor (-1/2 of C&A points awarded in question 6i ) | Subtraction of "1/2" C&A points |
| | | c | Failing ( -100% of C&A Points awarded in question 6i ) | Subtraction of 100% of C&A Points |

| FISMA<br>2004 Report Grading Elements | | | | |
|---|---|---|---|---|
| | | **Report Grading Element** | | **FY04 Possible Points** |
| **D. Configuration Management** | | | | **20** |
| **7** | | **Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?** | | |
| | | **1. Windows XP Professional** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | c | Between 71 and 80% | -0.5 |
| | | d | 70% and less or (No) | -1 |
| | | **2. Windows NT** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **3. Windows 2000 Professional** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **4. Windows 2000** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **5. Windows 2000 Server** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | **i)** | **6. Windows 2003 Server** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **7. Solaris** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **8. HP-UX** | | **0** |

| FISMA<br>2004 Report Grading Elements | | | | |
|---|---|---|---|---|
| Report Grading Element | | | | FY04 Possible Points |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **9. Linux** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **10. Cisco Router IOS** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **11. Oracle** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | c | 70% and less or (No) | -1 |
| | | **12. Other. Specify:** | | **0** |
| | | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -0.5 |
| | | d | 70% and less or (No) | -1 |
| | | **Do the configuration requirements implemented D.7.i address patching of security vulnerabilities?** | | **0** |
| | **ii)** | a | Between 81 and 100% or (N/A) | 0 |
| | | b | Between 71 and 80% | -4 |
| | | c | 70% and less or (No) | -8 |

| FISMA<br>2004 Report Grading Elements | | | | |
|---|---|---|---|---|
| | | Report Grading Element | | FY04 Possible Points |
| **E. Incident Detection and Response** | | | | **15** |
| **8** | | **The agency follows documented policies and procedures for reporting incidents internally** | | **4** |
| | **i)** | a | Between 96 and 100% | 4 |
| | | b | Between 81and 95% | 3 |
| | | c | Between 71 and 80% | 2 |
| | | d | Between 51and 70% | 1 |
| | | e | 50% and less | 0 |
| | **ii)** | **The agency follows documented policies and procedures for external reporting to law enforcement authorities.** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | **iii)** | **The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).** | | **2** |
| | | a | Between 96 and 100% | 2 |
| | | b | Between 81and 95% | 1.5 |
| | | c | Between 71 and 80% | 1 |
| | | d | Between 51and 70% | 0.5 |
| | | e | 50% and less | 0 |
| | **iv)** | **The percentage of systems that underwent vulnerability scans and penetration tests in FY04?** | | **7** |
| | | a | Between 90 and 100% | 7 |
| | | b | Between 75 and 89% | 5 |
| | | c | Between 60 and 74% | 3 |
| | | d | Between 45 and 59% | 1 |
| | | e | 44% and less | 0 |

| FISMA<br>2004 Report Grading Elements | | | | |
|---|---|---|---|---|
| | Report Grading Element | | | FY04 Possible Points |
| **F. Training** | | | | **10** |
| **9** | **The CIO has ensured security training and awareness of all employees, including contractors and those with significant IT Security responsibilities.** | | | **10** |
| | **i)** | **The percentage of agency employees (including contractors) and those with significant IT security responsibilities that received security training and awareness is:** | | **4** |
| | | *a* | Between 90 and 100% | 4 |
| | | *b* | Between 75 and 89% | 3 |
| | | *c* | Between 60 and 74% | 2 |
| | | *d* | Between 45 and 59% | 1 |
| | | *e* | 44% and less | 0 |
| | **ii)** | **The percentage of employees with significant security responsibilities that received specialized security training is:** | | **4** |
| | | a | Between 90 and 100% | 4 |
| | | b | Between 75 and 89% | 3 |
| | | c | Between 60 and 74% | 2 |
| | | d | Between 45 and 59% | 1 |
| | | e | 44% and less | 0 |
| | **iii)** | **The agency provided the total training costs for FY04.** | | **1** |
| | | a | Yes | **1** |
| | | b | No | **0** |
| | **iv)** | **The agency explains policies regarding peer-to-peer file sharing in IT security awareness training, ethics training or any other agency-wide training.** | | **1** |
| | | a | Yes | **1** |
| | | b | No | **0** |
| **G. Inventory (No deductions or -10 maximum)** | | | | **0** |
| **10** | **What progress has the agency made to develop an inventory of major IT systems. (Must have no deductions for 10i and 10ii or lose 10 pts)** | | | **0** |
| | **i)** | **The agency maintains an inventory of major IT systems and this inventory is updated at least annually.** | | **0** |
| | | a | Between 96 and 100% | 0 |
| | | b | 95% and less (Or the agency has no inventory) | -10 |
| | **ii)** | **The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.** | | **0** |
| | | a | Between 96 and 100% | 0 |
| | | b | 95% and less | -10 |